DATE(S) ISSUED:
07/10/2012

SUBJECT:
Vulnerability in Windows Shell Handler Could Allow Remote Code Execution (MS12-048)

OVERVIEW:
A vulnerability has been discovered in Windows Shell which could allow an attacker to take complete control of an affected system. The Windows Shell is used to run applications and manage the Windows operating system. Exploitation may occur if a user opens a file or directory which is specifically crafted to take advantage of this vulnerability. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability exists in Windows Shell because the shell does not properly handle file or directory names. An attacker could exploit this vulnerability by constructing a specially crafted file or directory and attempting to convince a user to open it from an email message or access it from a webpage. When a user opens the malicious file or directory, the Windows Shell will fail to properly handle the name and the attacker could execute arbitrary shell commands without the knowledge of the logged on user. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:
Microsoft:
http://technet.microsoft.com/en-us/security/bulletin/ms12-048

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0175

Security Focus:
http://www.securityfocus.com/bid/54307